UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/982,783	10/22/2001	David Henry Groves	WH-10 867US	8404

7590 04/08/2005

Dennison Associates
Suite 301
133 Richmond Street West
Toronto, ON M5H 2L7
CANADA

EXAMINER	
WILLIAMS, JEFFERY L	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 04/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/982,783	GROVES ET AL.	
	Examiner	Art Unit	
	Jeffery Williams	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 October 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 October 2001* is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☒ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Remarks

Claims 1 – 16 are pending.

The examiner makes note that the applicant has recited "a secure pin entry device comprising" in the preamble of claim 1. In line 11, the applicant recites "said secure pin entry device including:". The latter statement is unnecessary in view of the first.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 – 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hohle, "Methods and Apparatus for Dynamic Smartcard Synchronization and Personalization", U.S. Patent 6,199,762 B1 in view of Rankl et al., Smart Card

Handbook and further in view of Nordenstam et al., "Secure Distribution and Protection of Encryption Key Information", U.S. Patent 6,711,263 B1.

Regarding claim 1, Hohle discloses a system designed for establishing and updating a "pin entry device". The device of Hohle comprises an access point and a smartcard (IC card) designed to be used together (Hohle, col. 3, lines 35-37; col. 4, lines 9-21). The integration of a smartcard and access point enable the transmission of a PIN and other personal information to various institutions (Hohle, fig. 11). For example, it is disclosed that an IC card and a cellular phone may be used to interface with systems for the purpose of making transactions. Though Hohle discloses that the card and the access point can be physically separable, the purposed functionality is achieved through the combination of the two. Thus, it is obvious, such as in the use of a cellular phone containing a smartcard, to refer to the integration as a "pin entry device".

This conclusion finds support in Rankl et al., incorporated by reference by Hohle. Rankl et al. discloses that the smartcard (IC card) and access point must be combined (Rankl et al., pg. 307, par. 1). Similarly to Hohle, Rankl et al., demonstrates the combination of a smartcard contained by a cellular phone, referred singularly as a mobile station. This is disclosed as the foundation and standard for all later smartcard applications (Rankl et al., pg. 362-368).

Thus, it would have been obvious to one of ordinary skill in the art to combine the teaching by Rankl et al. of a smartcard and access point being a integrated, singular entity with the necessary combination of smartcard and access point as a "pin entry device" of Hohle, because the tight integration of the two components is necessary for the purposed functionality.

The combination of Hohle and Rankl et al. disclose:

a microprocessor (Hohle, col. 1, line 19);

memory (Hohle, col. 1, line 32);

secure memory (Hohle, col. 1, lines 30,31,33);

identification information (Hohle, fig. 11);

a communication capability (Hohle, col. 2, lines 37-41);

encryption software (Hohle, col. 10, lines 45-53). Hohle discloses that the smartcard contains various software applications stored in memory, and that transactions to and from the smartcard are securely implemented using cryptographic keys. Thus, it is obvious that the smartcard contains encryption software implementing the stored cryptographic keys to enable secure transactions from the card.

an activation program for completing a digital communication with an authorizing institute using said communication capability (Hohle, col. 13, line 57 – col. 14, line 4).

The combination of Hohle and Rankl et al. discloses that the pin entry device contains persistent memory, for the storage of user and operating data (Hohle, col. 1,

lines 29-35). Keys employed by the pin entry device are securely downloaded into the memory of the device (Hohle, col. 10, lines 59-64). The combination of Hohle and Rankl et al. disclose that transactions within the system can be secured and authenticated using public key algorithms, thus the combination discloses the use of public and private keys (Hohle, col. 4, lines 34-46). The combination of Hohle and Rankl et al., does not disclose the explicit downloading of public key into memory nor the downloading of a private key and digital certificate containing a public key into secure memory.

Nordenstam et al., discloses a smartcard used in a system employing a public key algorithm. Nordenstam et al. shows that the method of using public key cryptography includes storing a public key, private key, and a public key certificate into the secure memory of a smartcard (Nordenstam et al., fig. 2).

It would have been obvious to one of ordinary skill in the art to combine the key and certificate storage method of Nordenstam et al., with the combination of Hohle and Rankl et al. because the need to store a private and public keys and a certificate in secure memory is obvious with respect to smart cards utilized in public key schemes.

Thus, the combination of Hohle, Rankl et al., and Nordenstam et al. discloses:

a public encryption key stored in said memory, a private encryption key stored in said secure memory and a digital certificate which includes therein the public key and said identification information of said secure pin entry device

Regarding claim 2, the combination of Hohle, Rankl et al., and Nordenstam et al. discloses:

wherein said activation program includes a communication address to initiate a communication with the authorizing institute (Hohle, col. 5, lines 15-18). The authorizing institute is represented by the server side system comprising the "secure support client server" (104) and the supporting components.

Regarding claim 3, the combination of Hohle, Rankl et al., and Nordenstam et al. discloses:

wherein said secure pin entry device is ready for loading of financial keys and software from the authorizing institute using said encryption software and said public and private keys (Hohle, col. 3, lines 57-67; col. 6, lines 13-24; col. 10, lines 45-53).

Regarding claim 4, the combination of Hohle, Rankl et al., and Nordenstam et al. discloses:

a connection port for an electronic cash register system which forms part of said communication capability (Hohle et al., fig. 1, elems. 120,102,104). The pin entry device interfaces with the server for making transactions comprising transactions with financial institutions.

Regarding claim 5, the combination of Hohle, Rankl et al., and Nordenstam et al. discloses:

wherein said activation program includes information specific to a predetermined authorizing institute which the device will communicate with (Hohle, col. 5, lines 15-18). The pin entry device transmits information specifying the predetermined enterprise network with which it wishes to begin transactions.

Regarding claim 6 (AC), the combination of Hohle, Rankl et al., and Nordenstam et al. discloses:

wherein said device activation program is limited to a predetermined authorizing institute (Hohle, col. 5, lines 15-18). Communication is limited to "appropriate" destinations.

Regarding claim 7, the combination of Hohle, Rankl et al., and Nordenstam et al. discloses:

providing said secure pin entry device with personal identification information including a serial number, a private key, a public key, and a digital certificate provided by a Certificate Authority having a public key and a private key and wherein said digital certificate includes the public key of said secure pin entry device (Hohle, col. 3, lines 57-62; col. 10; lines 45-56; col. 11, lines 5-15). The key management system serves the function of the "Certificate Authority". As previously explained, Nordenstam et al. discloses that it is obvious that the transferred keying information include a public key, private key, and certificate.

locating said secure pin entry device in an operating location, forming a communication between said secure pin entry device and said authorizing institute and transmitting to said authorizing institute, said certificate (Hohle, fig. 1; col. 13, line 57 – col. 14, line 4; Nordenstam et al., Abstract). As disclosed, the pin entry device authenticates itself to the authorizing institute. The combination of Hohle, Rankl et al., and Nordenstam et al. discloses that the transfer of the certificate is an obvious part of the authentication process.

said authorizing institute confirming said certificate using the public key of said Certificate Authority (Hohle, col. 13, line 57 – col. 14, line 4). It is obvious that the authorizing institute confirms the authenticity of the certificate since it authorizes the access and updating of the device.

said secure pin entry device and said authorizing institute using said keys to encrypt and download confidential information received and deciphered by said secure pin entry device and used to program said secure pin entry device for secure communication with said authorizing institute (Hohle, col. 10, lines 59-64).

Regarding claim 8, the combination of Hohle, Rankl et al., and Nordenstam et al. discloses:

wherein said secure pin entry device and said authorizing institute use said keys to form a shared secret, and said shared secret is used to encrypt and decipher said confidential information used to program said secure pin entry device (Hohle, col. 10, lines 59-64). A shared secret is formed and used through the use of keys to secure the

communications. Such communications are considered secure because the keys are confidential to the parties communicating. Thus, a secret is shared.

Regarding claim 9, the combination of Hohle, Rankl et al., and Nordenstam et al. discloses:

wherein the step of providing said secure pin entry device with said private key and said digital certificate occurs in a secure environment (Hohle, col. 10, lines 59-64).

Regarding claim 10, the combination of Hohle, Rankl et al., and Nordenstam et al. discloses:

wherein said secure pin entry device is provided said private key and public key by an Initialization System and said Certificate Authority communicates with said Initialization System through a secure communication link (Hohle, col. 3, lines 57-65; col. 11, lines 5-14).

Regarding claim 11, the combination of Hohle, Rankl et al., and Nordenstam et al. discloses:

locating said Initialization System and said Certificate Authority in a common secure location (Hohle, fig. 9).

Regarding claim 12, the combination of Hohle, Rankl et al., and Nordenstam et al. discloses:

wherein said Certificate Authority and said Initialization System exchange public keys initially, and thereafter communication using encryption based on said keys (Hohle, col. 10, lines 40-67). The combination of Hohle, Rankl et al., and Nordenstam et al. discloses that the communicating parties involved in the transferring of keying material act in "accordance with a set of access condition rules". These rules stipulate the use of encryption between communicating parties. It is obvious, based upon logical reasoning, to realize that in order for encryption to take place in a public key system, the exchange of keys has to occur initially, and the usage of the exchanged keys must follow.

Regarding claim 13, the combination of Hohle, Rankl et al., and Nordenstam et al. discloses:

wherein the exchange of said public keys between said Certificate Authority and said Initialization System occurs only as required, and infrequently (Hohle, col. 3, lines 57-67).

Regarding claim 14, the combination of Hohle, Rankl et al., and Nordenstam et al. discloses:

wherein said confidential information includes financial keys and/or software (Hohle, col. 5, lines 25-36; col. 10, lines 40-48).

Regarding claim 15, the combination of Hohle, Rankl et al., and Nordenstam et al. discloses:

providing said secure pin entry device with information specific to the authorizing institute prior to locating said device whereby the device is specific to the authorizing institute (Hohle, cols. 11, 12).

Regarding claim 16, the combination of Hohle, Rankl et al., and Nordenstam et al. discloses:

providing said unique identification to an Initialization System (Hohle, fig. 1; col. 13, line 57 – col. 14, line 4; Nordenstam et al., Abstract). As disclosed, the pin entry device authenticates itself to the authorizing institute. The combination of Hohle, Rankl et al., and Nordenstam et al. discloses that the transfer of the certificate is an obvious part of the authentication process.

having said Initialization System provide said financial transaction device with a private key and a public key (Hohle, col. 3, lines 57-67; col. 10, lines 45-53; fig. 1).

forwarding to a Certificate Authority the financial transaction device public key and unique identification (Hohle, col. 11, lines 5-15). The "Certificate Authority" receives requests for the generation of keys. Such keys are generated with the information received from the initialization system.

producing at the Certificate Authority a digital certificate for said financial transaction device (Hohle, col. 11, lines 5-15);

providing said certificate to said financial transaction device (Hohle, col. 3, lines 57-67; col. 10, lines 45-53);

and storing said certificate in said financial transaction device (Hohle, col. 3, lines 57-67; col. 10, lines 45-53).

Regarding claim 17, the combination of Hohle, Rankl et al., and Nordenstam et al. discloses:

having said Initialization System provide said transaction device with a communication address of said Financial Institute (Hohle, col. 9, lines 58-67).

Regarding claim 18, the combination of Hohle, Rankl et al., and Nordenstam et al. discloses:

having said Initialization System provide said financial transaction device with an initiation program used to initiate a communication with said Financial Institute using said communication address (Hohle, col. 9, lines 58-67).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jeffery Williams
(571) 272-7965
4-1-05

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER